RESOLUTION R-020-23

A RESOLUTION OF THE WALKER COUNTY BOARD OF COMMISSIONERS TO AMEND THE EMPLOYEE ELECTRONIC PROPERTY AND COMMUNICATIONS SYSTEM POLICY

WHEREAS, the Board of Commissioners of Walker County ("Board") is the governing authority of Walker County, Georgia; and

WHEREAS, the Board has determined it is desirable and necessary to update the county's Employee Electronic Property and Communications System Policy to clarify the responsibility of each employee concerning the use of county computers and networks; and

THEREFORE BE IT RESOLVED by the Board of Commissioners of Walker County, Georgia that the Walker County Government Employee Electronic Property and Communication Systems Policy, attached hereto marked "Exhibit A," and incorporated by reference, is hereby adopted and shall be implemented immediately.

BE IT FURTHER RESOLVED any other Resolution or county policy addressing the use of county computer and network systems prior to this date, that is now in conflict with any of the provisions of this Resolution, is hereby repealed.

SO RESOLVED this 13th day of April, 2023.

ATTEST:

Whitney Summey

Whitney Summey Deputy Clerk

WALKER COUNTY, GEORGIA

SHANNON K. WHITFIELD, Chairman

The foregoing Resolution received a motion for Passage from Commissioner Bickemore, second by Commissioner Hart, and upon the question the vote is 4 ayes, 0 nays to adopt the Resolution.

ELECTRONIC COUNTY PROPERTY AND COMMUNICATION SYSTEMS

Statement of Policy

The County provides a variety of channels for communication to promote the efficient operation of its business. All communications transmitted by, received from, or stored in these systems are the sole property of Walker County and an employee should have no expectation of privacy related thereto. All electronic communication systems, supplies, equipment, computers, disk drives, information, and any other material or electronic County property obtained and used during the course of employment (regardless whether during normal working or non-working hours) is exclusively owned by Walker County.

Employees should immediately report any violation of this policy to their Elected Official/Department Head and/or the Information System/Technology (IT) Director. The Information System/Technology Director shall notify the Human Resources (HR) Director of suspected violations of this Policy. Violations of any section of this policy will result in disciplinary action up to and including termination.

Monitoring of Electronic Communication Systems

IT system monitoring will take place where appropriate, and investigations will be conducted when reasonable suspicion exists of a breach of this or any other policy. Periodic monitoring of activity on County systems, including internet and email use, is appropriate to ensure security and effective operation, and to protect against misuse.

Any electronic communication system usage may be monitored at any time at the discretion of the Human Resources Director along with the Information System/Technology Director. These situations should normally be limited ~~restricted~~ to internal investigations or official investigations, such as for law enforcement proceedings. However, there may exist situations where a review is warranted prior to the formal commencement of an investigation or where the interests of the County will be materially advanced by such a review. IT and HR staff may be involved as needed and at the determination of the Human Resources Director and the Information System/Technology Director. Any monitoring exercises will exclude involvement by Managers, Directors, Elected Officials and their staff. ~~The Human Resources Director will report findings to the Board of Commissioners.~~ The Human Resources Director shall report the outcome of such an inquiry and review to the appropriate Elected Official.

The Information System/Technology Director and Human Resources Director are authorized to oversee and manage all County communication systems. To facilitate that role, the Information System/Technology Director may draft and recommend additional policies to the Board of Commissioners. ~~create additional and detailed policies consistent with this Policy, which policies shall be complied with by employees upon distribution of the same.~~ A copy of all approved ~~any such~~ policies ~~promulgated by the Information System/Technology Director~~ shall be maintained in the Human Resources Department. ~~The Information System/Technology Director shall immediately notify reported suspected violations of this policy to the Human Resources Director.~~

The burden of responsibility is on the employee to abide by this Policy and, prior to use, inquire about specific uses not cited. It is the employee's responsibility to report suspected breaches of security policy without delay to your Department Head, the IT department, or an Elected Official. All breaches of information security policies will be investigated. For any and all questions on topics not covered please inquire with your supervisor or the Information Systems and Technology Department.

System Security

Employees are responsible for the use of their accounts and the security of their passwords. Employees may not give anyone access to his/her account, or use a County computer account assigned to another user. The only exceptions would be to share the username with an employee of the IT Department for support and maintenance or if the account was established as a shared account. A user must not attempt to obtain the password of another employee. If an employee suspects someone knows his/her password, the employee should change the password and contact their Elected Official/Department Head and the IT Director immediately.

Employees cannot use the computer or network resources of the County to gain or attempt to gain unauthorized access to remote computers, networks, or systems, nor shall they attempt to circumvent data protection schemes or exploit security loopholes. Employees may not place on any County-owned computer or network system any type of information or software that gives unauthorized access to another computer account, system or network. Employees shall not load any software on County computers, nor connect flash drives or other removable media from unknown sources on County-owned systems, networks or any other electronic devices. This includes but is not limited to, programs known as computer viruses, such as a trojan horse, worms, trap-door program code, ransomware, or other code or files designed to disrupt, disable, impair, render inaccessible, or otherwise harm either the County's networks/systems or those of any other individual or entity.

The County has established a Secure Network at each County office facility that is password protected. Only County provided devices should be connected to the Secure Network. All devices not issued by the County should connect to the internet using only the Guest Wi-Fi Network, which doesn't require a password. The Guest Wi-FI Network is also available for all citizens or guests that need access to the internet.

Mobile Phones

County ~~cellular phones/Smartphone~~ mobile devices, including, but not limited to phones and tablets, are provided to key individuals for the purpose of ensuring accessibility and enhancing individual efficiencies in handling County business. ~~Cellular phones are not a personal benefit and are not intended for use as a primary mode of personal communication.~~

Excessive use of a personal mobile device ~~cellular phone~~ while on County duty may result in disciplinary action. Elected Officials/Department Heads~~Directors~~ have the authority to restrict or prohibit the use of any mobile device, County supplied or personal, at any time while an employee is on the job if it is determined that use of a mobile device presents a safety hazard or distracts from the duties of the job.

Employees are permitted to use a mobile phone while driving, only if the vehicle is equipped with a "hands-free" system. Employees who do not have a "hands-free" system should park in a safe area before making or receiving calls, texting, emailing or otherwise using a mobile device.

Integrity, Encryption, Storage and Backup of Data

In order to provide users with a reliable and secure means of storing and saving work-related data in the cloud, the County IT Department has implemented the Google Drive data storage solution. By saving work-related data to a Google Drive folder or Google Drive shared folders, the County IT Department can help ensure the confidentiality, integrity, availability, and encryption of the data.

All County data files are required to be stored in Google Drive folders to insure data integrity, data backup, and encryption of data. Files stored on any local computer drive, including your computer's C drive or desktop, are not backed up or encrypted by the County's IT Department. No assurance for reclaiming lost work-related data stored on local drives or desktops can be offered by the IT Department. Any work-related data stored or saved to a local drive or desktop is done so at the user's own risk. Contact the IT Department if you have any questions regarding this policy.

Specifics on Computer and Network Usage

~~a) Responsible Use of Resources~~
~~You are responsible for knowing what information resources (including networks) are available, remembering that the members of the community share them, and refraining from all acts that waste or prevent others from using these resources or from using them in whatever ways have been proscribed by the Walker County Board of Commissioners and the laws of the state and federal government.~~

~~b) Use of Computer Devices~~
~~You are responsible in coordination with your Department Director for the security and integrity of Walker County information stored on your computer devices. This responsibility includes making regular disk backups and controlling physical and network~~

~~access to the machine. Avoid storing passwords or other information that can be used to gain access to other government computing resources.~~

a) Access to Facilities and Information

1) Sharing of Access
Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. You are responsible for any use of your account.

2) Permitting Unauthorized Access
You may not install or otherwise configure software or hardware to intentionally allow access by unauthorized users.

3) Use of Privileged Access
Special access to information or other special computing privileges are to be used in performance of official duties only. Information that you obtain through special privileges is to be treated as private.

~~4) Attempts to Circumvent Security~~
~~Users are prohibited from attempting to circumvent or subvert any system's security measures. This section does not prohibit use of security tools by system administration personnel.~~

5) Decoding Access Control Information
You are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

6) Denial of Service
Deliberate attempts to degrade the performance of a computer system or network or to deprive authorized personnel of resources or access to any Walker County computer system or network are prohibited. This includes but is not limited to, tampering with components of a local area network (LAN) or the high-speed network, otherwise blocking communication lines, or interfering with the operational readiness of a computer.

7) Harmful Activities
The following harmful activities are prohibited: creating or propagating viruses; disrupting services; damaging files; intentional destruction of or damage to equipment, software or data belonging to Walker County ~~Board of Commissioners~~ or other users; and the like.

8) Unauthorized Monitoring
You may not use computing resources for unauthorized monitoring of electronic communications.

9) Government Dishonesty
You should always use computer resources in accordance with high ethical standards and in correspondence with local, state and federal law.

10) Use of Copyrighted Information and Materials
You are prohibited from using, ~~inspecting,~~ copying, and storing copyrighted computer programs and other materials, in violation of copyright laws.

11) Use of Licensed Software
No software may be installed, copied, or used on Walker County resources except as permitted by the owner of the software. Software subject to licensing must be properly licensed and all licensed provisions (installation, use, copying, number of simultaneous users, terms of license, etc.) must be strictly adhered to. Any and all new software installations must be approved in some form by the County's ~~designated network and computing personnel~~ Information System/Technology Director.

12) Political Campaigning; Commercial Advertising
The use of system materials, supplies, equipment, machinery, or vehicles in political campaigns is forbidden. Political campaigns and commercial advertisements shall not be intentionally displayed on government property. The use of County computers and networks shall conform to these policies.

13) Personal Business
~~Computing facilities, services,~~ Computers, servers and networks may not be used in connection with compensated outside work or for the benefit of organizations not related to the business of the County. Any other incidental use (such as electronic communications or storing data on single-user machines) must not interfere with other users' access to resources (computer cycles, network bandwidth, disk space, printers, etc.). State law restricts the use of state facilities for personal gain or benefit.

~~**Internet and Email Conditions of Use**~~

~~All employees will be assigned an internet access usage level by their Constitutional Officer/Department Head when hired. Use of Walker County Government internet and email is intended for business use. Personal use of the internet or email is permitted where such use does not affect the individual's business performance, is not detrimental to Walker County Government in any way, is not in breach of any term and condition of employment and does not place the individual or Walker County Government in breach of statutory or other legal obligations. All individuals are accountable for their actions on the internet and email systems.~~

Prohibited Uses of the Internet

Viewing, sending, receiving, displaying, printing, or otherwise disseminating material that is fraudulent, harassing, illegal, embarrassing, sexually explicit, offensive, obscene, intimidating or defamatory is prohibited.

Reporting Child Pornography

Any employee who witnesses child pornography being viewed or distributed on any County owned device is responsible for immediately reporting it to his or her Elected Official/Department Head. This also applies to employee-owned devices which are used on County property. The Elected Official/Department Head will immediately inform the County Attorney and Human Resources department, which will take prompt appropriate remedial action. Personnel excluded from this policy include the Prosecutor's Office, the Sheriff's Department, and other limited personnel involved in the investigation and prosecution of these illegal acts.

Child pornography includes any visual depiction or description of a child, less than eighteen (18) years of age, engaged in sexually explicit conduct, including the nudity of a child. Child pornography, whether made or produced by electronic, mechanical, or other means, may be expressed through a picture, drawing, photograph, negative image, undeveloped film, motion picture, videotape, digitized image, or any other pictorial representation.

Moreover, any employee who makes available to another employee a computer, knowing that the computer's fixed drive or peripheral device contains matter that depicts or describes sexual conduct by a child less than eighteen (18) years of age commits child exploitation.

Electronic Mail (E-mail) - GA Open Records Laws

Employees should exercise care when drafting e-mail communications. Employees should not reveal any personal information when drafting e-mail, such as a home address, home phone number, or phone numbers of other individuals. An employee's e-mail signature must only use County contact information. **The County e-mail system is subject to Georgia Open Records laws and may be deemed as public records. Employees should not conduct County business from private email accounts.**

Social Media Use and Guidelines

The role of technology in the workplace is constantly expanding and now includes social media communication tools that facilitate interactive information sharing, interoperability, and collaboration. Commonly used social media platforms, including Facebook, Twitter, YouTube, Instagram, and LinkedIn, have large, loyal user bases and are an increasingly important outreach and communication tools for government entities from the federal to the local level. The Walker County IT department will block access from County networks to any social media or websites that are listed as a threat to National Security by Cybersecurity & Infrastructure Security Agency (CISA).

Walker County has an overriding interest in deciding what is "spoken" on behalf of the County on social media sites. This includes, but is not limited to, the creation of Walker County social media accounts and posting information or commenting on social media about county related business. Team members not authorized to comment publicly should refrain from communication that could be perceived as representing a formal response from the County.

As such, the Walker County Public Relations Director will regulate access to all authorized social media outlets. Employees given access to Walker County social media platforms should consult the County Public Relations Director before making any post or comment that might be considered outside of the normal day-to-day communication. In addition, social media users should be aware these types of communications are considered public records and, consequently, must comply with the Georgia Open Records law. Employees should immediately report any violation of this policy to their Elected Official/Department Head and/or the IT Director.

Separate Personal & Professional Accounts

Employees should be mindful of blurring their personal and professional lives when posting on social media. While employees are permitted to have personal social media accounts, these accounts must remain personal in nature. Employees should be aware they run the risk of having their personal social media accounts subject to Georgia Open Records laws when making posts or comments about County related topics or issues.

Employees should not speak for or on behalf of the County when utilizing personal social media accounts. Employees may not post anything in the name of the County or make statements that could reasonably be attributed to the County or any Elected Official. Employees should refrain from rendering opinions or political views on behalf of the County or any Elected Official. Similarly, employees who appear in a video commenting on County issues or policies should preface their comments by making it clear that the employee is not speaking on behalf of the County and that any opinions reflected therein do not reflect the views of the County or any Elected Official. In addition, employees should never use their county e-mail account or password in conjunction with a personal social networking site.

County employees should not post communications that may constitute knowingly false or malicious comments, discriminatory remarks, sexual or racial harassment, hostility based on age or disability, threats of violence, sabotage, or other similar or related unlawful conduct. Employees should not post communications that may divulge confidential information. Employees should immediately report any violation of this policy to their Elected Official/Department Head and/or the IT Director.

Social Media Guidelines

Walker County encourages employees who use social media to follow the below guidelines:

1. Do not post any comment or picture involving an employee, volunteer, department, or other County entity without their express consent. This guideline does not apply to those authorized to manage County social media platforms.

2. If an employee posts any comment about the County, the employee must clearly and conspicuously state that he/she is posting in their individual capacity and that the views posted do not represent the views of the County.

3. Unless given written consent, an employee may not use the County's logos or any organizational material in their posts.

4. All postings on social media must comply with the County's policies on confidentiality and disclosure of proprietary information.

5. Employees are responsible for what is written or presented on social media. The posting party can be sued by other employees or any individual that views the social media posts as defamatory, harassing, libelous, or creating a hostile work environment.

7. All organizational policies that regulate off-duty conduct apply to social media activity including, but not limited to, policies related to illegal harassment, code of conduct, non-discrimination, and protecting confidential and/or proprietary information.

8. When creating social media accounts that require individual identification, County employees should use their actual names and should not communicate or imply any affiliation or relationship with the County.

9. The County's policy on the Use of Information Technologies, the Internet, and E-Mail applies to social media use at work, including the County's policy regarding personal use on all County-issued electronic devices.

Using Social Media at Work

Employees should limit social media use while on work time or while using County provided devices/computers unless it is work-related and authorized by your Elected Official/Department Head. Social media use should not distract an employee from the duties of their job. Employees should not use their County provided e-mail address to register on social networks, blogs, or other online tools utilized for personal use.

Authorized County Social Media Communications

Authorized County employees who manage County social media platforms should communicate in a professional manner and should always conduct business in accordance with the department's communications policy, practices and expectations.

Social media accounts associated with Walker County Government and managed by authorized employees should refrain from the expressions of personal opinions, dissemination of political views, advocacy of violence or illegal activity, or be used for non governmental purposes. Employees should conduct themselves according to the highest ethical standards. If an employee is uncertain about the appropriateness of a social media posting, check with the County Public Relations Director.

Walker County generally uses social media to 1) disseminate time-sensitive information as quickly as possible (for example emergency information), 2) to publicize public meetings to the residents of the County, and 3) provide information on County services and items of public interest. Wherever possible, content posted to the County's social media accounts or sites will also be available on the County's website. Wherever possible, content posted to Walker County social media sites should contain links directing users back to the County's website for in-depth information, forms, documents, or online services necessary to conduct business with the County.

There should be great care and consideration when communicating by way of social media. In this regard, County employees, Elected Officials, and/or Department Heads must not knowingly communicate inaccurate or false information. All reasonable efforts should be made to provide accurate and factual information.

Handling of Sensitive and/or Confidential Data ~~Clear Desk and Clear Screen Policy~~

In order to reduce the risk of unauthorized access or loss of information, employees should be mindful of their handling of sensitive and/or confidential data: ~~Walker County Government enforces a clear desk and screen policy as follows:~~

- Personal or sensitive and/or confidential business information must be protected using security features provided.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care ~~Case~~ must be taken to not leave sensitive and/or confidential material on printers or photocopiers. All business-related printed matter must be retained or disposed of according to its appropriate retention schedule. ~~disposed of using confidential waste bins or shredders.~~

Working Off-Site

It is accepted that mobile devices, such as laptops, mobile phones, smartphones, and tablets, will be taken off-site. Information should be protected against loss or compromise when working remotely (for example at home or in public places). Mobile devices should be handled in a secure manner and locked when not in use. Additionally, mobile devices and media taken off-site must not be left unattended in public places and not left in plain sight in a vehicle. (Exempt: equipment mounted in county vehicles)

The provisions of this Policy shall be applicable when mobile devices are used off-site. ~~The following controls must be applied:~~

- ~~Working away from the office must be in line with Walker County Government remote working policy.~~

- ~~Equipment and media taken off-site must not be left unattended in public places and not left in sight in a vehicle car (Exempt: equipment mounted in vehicles). exceptions for law enforcement maps apply).~~
- ~~Laptops must not be placed in storaged luggage during travel. carried as hand luggage when traveling.~~
- ~~Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.~~
- ~~Particular care must be taken with the use of mobile devices such as laptops, mobile phones, smartphones, and tablets. They must be protected at least by a password or a PIN and, where available, encryption.~~

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs, and removable hard drives must be only used in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only ~~the~~ County authorized mobile storage devices with encryption should be used ~~enabled to be used~~ when transferring sensitive or confidential data. ~~Failure to comply with these provisions will result in disciplinary action up to and including termination.~~

~~**Software**~~

~~Employees must use only software that is authorized by Walker County Government on Walker County Government computers. Authorized software must be used in accordance with the software supplier's licensing agreement. All software on Walker County Government computers must be approved and installed in the Walker County Government IT Department.~~

Viruses & Downloading from the Internet

The IT department has implemented centralized, automated virus detection and virus software updates within the ~~Walker~~ County ~~Government~~. All PCs have antivirus software installed to detect and remove any virus automatically. Individuals should not attempt to remove or disable the anti-virus software. All material downloaded from the internet or from computers or networks that do not belong to the County MUST be scanned for viruses and other destructive programs before being placed onto a County computer or the secure network system. Do not attempt to install free software downloaded from the internet and/or software brought in from home. Prohibited examples include iTunes, screensavers, Internet Explorer toolbars, games, etc. All employees are expected to follow the instructions of the IT Department for proper scanning and/or downloading.

Employees should not download and store personal files on County equipment. This includes but is not limited to music, pictures, or videos. Any personal files found stored on County equipment will be removed without warning and will not be recoverable. Employees are responsible for the material they review and download on the internet.

~~**Telephone (Voice) Equipment Conditions of Use**~~

~~Use of Walker County Government voice equipment is intended for business use. Individuals must not use Walker County Government voice facilities for sending or receiving private communications on personal matters, make hoax or threatening calls or accept reverse charge calls for personal reasons from domestic or International operators. All non-urgent personal communications should be made at an individual's own expense using alternative means of communication.~~

Actions upon Termination

All ~~Walker~~ County ~~Government~~ equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to the ~~Walker~~ County ~~Government~~ at termination of employment. All ~~Walker~~ County ~~Government~~ data or intellectual property developed or gained during the period of employment remains the

property of the ~~Walker~~ County ~~Government~~ and must not be retained beyond termination or reused for any other purpose.

When you cease being a County employee, ~~member of the government community,~~ or if you are assigned a new position and/or responsibilities within the County, your access authorization must be reviewed. You must not use facilities, accounts, access codes, privileges, or information for which you are not authorized in your new circumstances.

~~Failure to comply with all of the provisions within this policy will result in disciplinary action up to and including termination.~~